Securing OT against Log4j; Is it really a thing?

By Marty Edwards, VP OT Security & Michael Rothschild, Senior Director, OT Solutions

By now you are well familiar with CVE-2021-44228. The Log4j vulnerability is being categorized as one of the most pervasive and potentially far reaching vulnerabilities in history. Log4j is an open source Java logging library used extensively by developers. First appearances are that this is an IT issue that cannot impact OT environments; but in fact Apache and thus Log4j is embedded in operational technology (OT) environments. In fact, many organizations have converged their IT and OT operations thereby making lateral creep of attacks between the two increasingly common. Even if your facility is fully air-gapped, there is a better than average chance that you may be "accidentally converged", thus putting your operation at risk.

Here are five key actions to take right now to secure your OT environment against Log4j:

1. **Follow official guidance.** Organizations such as the U.S. Cybersecurity and Infrastructure Security Agency (CISA) have issued specific guidance. It is crucial to be familiar and follow this guidance on an ongoing basis. Compliance with, and reliance on, frameworks from MITRE, the U.S. National Institute of Standards and Technology (NIST), the U.K. Network and Information Systems (NIS) and the North American Electric Reliability Corporation (NERC) can help your organization establish best practices in order to stay vigilant against dynamic threat conditions.
2. **Know your assets.** Asset inventory is a cornerstone of any security program and can provide deep situational awareness. It involves more than capturing the make-and-model of everything in your environment. It requires having an up-to-date inventory of firmware versions, patch levels, communication paths, access and much more. Network monitoring alone will only provide some of the detail. A combination of network and device-specific querying is necessary in order to get the specifics.
3. **Run a targeted scan of IT assets.** Once you have a good asset inventory, you should be able to run a vulnerability scan to see where else you may be impacted. Keep in mind that up to 50% of your OT environment contains IT assets including HMIs, IIoT devices, routers, servers switches and more. You'll need Log4j signatures for detecting the specific exploit and at-risk elements.
4. **Understand your OT exposure.** Now that you've checked your IT assets, it is imperative to check your OT assets as well. You'll need an OT security solution that can specifically address the unique properties and conditions that are prevalent in OT environments. It is ill advised to use the same scanning tool that you used for IT in your OT environment since the two worlds, while converging, behave very differently.
5. **Be proactive in reducing risk.** If you are relying only on intrusion detection alerts to warn you of a compromise or an exploited system, it is already too late. Ongoing threat assessments, what is often referred as proactive cyber-maintenance must involve the

most up-to-date intelligence, sources and tools. The ability to find risky behaviors, configurations and activity and preempt attacks is a best practice for keeping your operations running without compromise.

The manufacturing and critical infrastructure community needs to improve its understanding of what is being used within systems in order to achieve the deep situational awareness required to address new threats as they emerge in the wild. The Software Bill of Materials (SBOM) initiative was directed by Executive Order issued in May 2021. An SBOM can provide end users the transparency required to know if their products rely on vulnerable software libraries.

There is no doubt that we will be dealing with the Log4j vulnerability for years to come and, unfortunately, there will undoubtedly be other vulnerabilities in the future. With the right people, processes and technologies in place, organizations around the world can quickly and collectively use risk-based decision making to minimize the consequences of vulnerabilities like Log4jand protect the world’s critical infrastructure.